Information Technology Industry Council

Written Testimony of

Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the

Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives

The Expanding Cyber Threat

January 27, 2015

Written Testimony of:
Dean Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the:
Subcommittee on Research and Technology
Committee on Science, Space, and Technology
U.S. House of Representatives

The Expanding Cyber Threat

January 27, 2015

Chairwoman Comstock and members of the subcommittee, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before the Subcommittee on Research and Technology on the important topic of cybersecurity. We welcome your interest and engagement on this subject.

ITI is the global voice of the leading technology companies from all corners of the information and communications technology (ICT) sector, including hardware, software, and services—the majority of whom are based here in the United States. Cybersecurity is critical to our members' success—the protection of our customers, our brands, and our intellectual property are essential components of our business and our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity.

In addition, as both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. That's important to keep in mind because when it comes to cybersecurity, our connectedness is through an Internet that is truly global and borderless. We acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and lead – global norms.

I will focus my testimony on four areas: (1) The cybersecurity challenges facing our society today; (2) how industry's response to cyber threats and challenges has evolved from the start and will continue to do so; (3) how our industry sees the future of cybersecurity; and (4) how the federal government can partner with industry, or assist our work, in protecting our assets from successful cyber-attacks.

The Cybersecurity Challenges Facing Us Today

As you have heard from the other panelists, the threats and challenges are certainly many, they continually evolve, and are becoming more sophisticated.

For example, a key challenge facing us now are advanced persistent threats (APT), which use

multiple phases to break into a network, avoid detection, and harvest valuable information over the long term. APTs differ from traditional threats in that they are targeted, persistent, evasive and extremely advanced. Although there are many challenges in addition to APT, there is a common theme—our cyber adversaries are becoming more and more intelligent, creative, and resourceful. These challenges do not just face American industry, but industry globally, and they impact citizens and our use of the Internet and e-commerce.

But I want to stress that not all cybersecurity threats are, or should be, of equal concern. The risks to all companies, government agencies, or citizens are inherently different because threats do not impact all of us the same way—if at all.

The risk differs by entities, depending on industry, size, and assets. Banks face different risks than manufacturers, hospitals, railroads, or movie studios. Some industries are targeted for money, others for personal data, others for confidential business information, such as trade secrets, that can help a competitor bring a product to market faster or allow them to get the upper hand in business negotiations. The threat of an organized crime syndicate seeking credit card numbers is more pertinent to an online commerce company or bank than a steel manufacturer, for example. A global bank headquartered on Wall Street will likely be a bigger target than a corner bank in a small town. Individuals at home are much less likely than companies to be the target of an advanced persistent threat. The threat may not even be a sophisticated one at all. Unpreparedness or simple error can make a gateway for the worst havoc.

When it comes to cybersecurity, one size does not fit all. The varying challenges underscore why the best approach is a system in which entities are empowered to manage their own cybersecurity risks. Each entity has a distinct risk, and needs to allocate their cybersecurity resources in their own unique way depending on what their "crown jewels" are, where they are kept, and who might want them. Our sector's innovation allows us to create products and services for all stakeholders to identify, manage, and mitigate their ever-changing risks.

ICT Industry Evolving Responses to Cyber Threats and Challenges

The ICT industry is improving cybersecurity in two distinct and important ways: via the products and services we make, and the cybersecurity risk management practices we employ and promote.

In the products and services realm, we are innovating technologies to counter and stop criminals that are increasingly able to penetrate companies' information technology (IT) systems. We are also making security easier to use and investing in managed security services. In terms of corporate cybersecurity risk management, ITI's members are major, multinational companies that have managed cybersecurity risks for decades.

Our products and services to improve security. ITI's member companies—and the global ICT industry generally—have innovated and invented security for decades. It is important to stress that the real advancements in security are not large and splashy, however. Like our bodies' immunity system, there are millions of small innovations that accumulate and come together piece-by-piece to make security more pervasive in our interconnected lives and economies. And

these millions of innovations are driven by our companies, as well as thousands of new entrepreneurs and companies around the world, inventing in this space.

Like a collaborative network, the growing marketplace helps all of us deal with hackers, conduct remediation, and build skills. Enabling all of these inventions is our commitment to research and development (R&D). ITI companies invest incredible amounts in R&D. In fact, many ITI member firms have annual R&D budgets orders of magnitude greater than that of the Defense Advanced Research Project Agency (DARPA), which is renowned as our government's incubator for new technologies like networked computing. Given that DARPA's FY2014 R&D budget was $2.9 billion, our member companies are investing a staggering sum.

I am sure Members of the Committee are familiar with some of the more widely known security technologies that have evolved and captured the spotlight over the past few years. These included firewalls to protect the perimeter of your computer or network, anti-virus software to detect and remove computer viruses, and intrusion detection software (to figure out if a network had been breached), or intrusion prevention software (to try to predict and prevent being breached). These types of technologies evolved to meet changing threats and risks and continue to evolve.

Using sophisticated analytics to detect and react to anomalies. The technologies I mentioned above are just the tip of the innovation iceberg, and we are beyond the stage where firewall defenses are adequate. Each time we "up our game," hackers innovate in tandem to get around such defenses. Thus, the ICT industry has created and uses sophisticated data analytic software to monitor data, learn what is normal or aberrant, identify suspicious or anomalous activities, and react in real-time, such as by quarantining data before it can be exfiltrated. Companies also use data analytics to spot and tackle issues like fraud. And our innovations are certainly not only in products; we also innovate security services.

Making security the default norm, and easier to use. The reality is most security incidents involve some kind of human error: use of weak passwords, an employee clicking on spam and inadvertently downloading malware that hijacks a computer hard drive and exfiltrates valuable data, or inadequate network management that does not appropriately segment and section off data to those who truly need to access it.

Some of the most high profile cases over the past several months have shown how criminals are exploiting human weaknesses or mistakes made by users. One reason these mistakes happen is that security, particularly online, is difficult, complex, and time-consuming, and it is human nature to try to avoid things that are complex and take time.

To address this weak link, ICT companies are making it easier for the user to enable their own secure environments. This means we are creating products where security features such as encryption are turned on by default. Some smartphones now come with fingerprint readers in lieu of passwords to allow access. What used to be the realm of science fiction or blockbuster films are now in a phone that you can buy for a few hundred dollars.

Ensuring more experts are managing security. Our companies are also helping to make security the responsibility of experts who know how to handle it. This is happening as we migrate to managed technology services where an IT system is maintained by an outside vendor as a service-based contract, and security is built into the contracts. In the service-based world, the service provider and its cybersecurity experts remain part of that relationship and have the incentive to have a secure and resilient network. If, because of a security incident, a managed service provider's IT system is down and unable to serve customers, the provider will face financial consequences.

Our corporate cybersecurity risk management practices. ITI's members are major multinational companies that have understood and managed cybersecurity risks for decades. Our companies build risk management into their ongoing daily operations through legal and contractual agreements, cybersecurity operational controls, cybersecurity policies, procedures, and plans, adherence to global risk management standards, and many other common practices. Many operate 24-hour, 7-day-a-week network operations centers (NOCs) and participate in a host of entities that help them to understand and manage their risks, such as Sector Coordinating Councils (SCCs) and information sharing and analysis centers (ISACs). We are confident that many large, multinational companies are similar to ITI companies in these ways.

One very useful tool I want to highlight is the Framework for Critical Infrastructure Cybersecurity (Framework) released by the National Institute of Standards and Technology (NIST) in February 2014.

The Framework has great potential to help individual organizations manage their cyber risks, collectively strengthening our nation's cybersecurity. It represents an effective approach to cybersecurity because it leverages public-private partnerships, is based on risk management, and is voluntary. It references existing, globally recognized, voluntary, consensus-based standards, and best practices that are working effectively in industry now. It is technologically neutral, fostering innovation in the private sector and allowing industry to nimbly meet ever-changing cybersecurity challenges. And it nicely articulates how organizations should be factoring privacy considerations into their cybersecurity activities.

Importantly, the Framework is flexible, recognizing that different types of entities may use it for different purposes. Although it is aimed at critical infrastructure owners and operators, it can be useful to entities regardless of their size or relevance to U.S. national and economic security.

The process that went into developing this Framework has been a model for how the public and private sectors can work together to serve the national interest. In effect, the U.S. Government leveraged a tremendous amount of stakeholder input in an open, transparent, and collaborative manner, to create a major cybersecurity policy initiative. Government, industry, and other private stakeholders have a shared interest in improving cybersecurity, and the Framework moves us significantly toward that goal.

The Future of Cybersecurity and Our Top Concerns

We see the threat becoming greater and more persistent, and constantly changing. Our efforts

will continue to evolve in tandem. We believe our efforts both in inventing security technologies and services, as well as in managing risks to the security of our networks, are effective approaches to cybersecurity.

But we should all be clear: there is no silver bullet to cybersecurity, and there never will be. For every new defense, there will be an adversary bent on breaching it. The beauty of technology and the Internet—that technologies and business models constantly evolve—means that targets, and attack methods, will constantly change too.

Our efforts aim to reduce the effectiveness of attack methods, and we invest in technology, processes, and education to eliminate human error as much as possible. Our goal is managing our risks and becoming resilient. And that is something we are doing very well. But this is a long journey that does not have an end.

Frankly speaking, a key concern of the ICT industry as we continue to constantly improve cybersecurity is that overbroad and inflexible policies will hamper our ability to innovate or prevent us from changing course when needed to meet dynamic threats. This isn't hyperbolic. The technology sector can point to scores of laws that were crafted in a different age that are incapable of keeping up with technology. That is not the course anyone should want when it comes to securing our connected world. In fact, the current, non-regulatory, non-prescriptive approach to cybersecurity policy in the United States that allows the most innovative minds in industry to lead and respond to the changing cyber threat is one that should not be altered.

How the Government Can Be Helpful

As policymakers, your interest in getting cybersecurity policy right is welcomed and encouraged. However, governments must resist thinking that just because there is an incident online that government must be the first responder. As I have outlined above, companies are making investments, and more and more executives are focused on solving the problems.

Working with all stakeholders, including governments, we are well-positioned to manage these risks. To compliment and enable industry efforts, U.S. government efforts should focus on:

- **Supporting federal agencies' outreach on the Framework.** ITI strongly supports the Framework for Improving Critical Infrastructure Cybersecurity, and believes Congress should allow further time for it to enhance cybersecurity practices. Congress can help the Framework achieve its goals by ensuring NIST, the Department of Homeland Security, and other relevant departments have the funding they need to conduct ongoing and extensive outreach and awareness about the Framework.

- **Continuing government funding for cybersecurity research and development (R&D).** I noted earlier that our companies invest strongly in cybersecurity R&D. We will continue to do so. But federal investments will remain essential, because we count on the government to perform R&D that simply is not viable for the private sector. By necessity, companies' R&D efforts tend to be commercially focused. We need the government to fund early-stage, high-risk research that can create breakthrough

technologies and new market segments. The government can also look out over a longer time horizon, helping to set our R&D long-term sights correctly. The Cybersecurity Enhancement Act of 2014, which became law late last year, is an important down payment on government-supported R&D. For example, we look forward to reviewing the cybersecurity R&D strategic plan that will enable federal agencies to have a more unified approach to cybersecurity and information technology R&D. We hope those efforts take a similar approach to the development of the Framework by including a robust public-private engagement.

- **Continuing government efforts to raise awareness.** Government should work to raise awareness among users of technology (individuals of all ages and businesses of all sizes) about their cybersecurity risks and empower all stakeholders to understand and act upon their roles and responsibilities. In any awareness-raising, governments should partner with the private sector, which has already invested substantially in such efforts. The Cybersecurity Enhancement Act of 2014 also made strides in this area. Cybersecurity competitions and challenges for students, universities, veterans and other groups to recruit new cybersecurity talent, a cybersecurity scholarship for service program for individuals to help meet the needs of the federal government's cybersecurity mission, and the National Cybersecurity Awareness & Preparedness Program are also parts of a growing and effective education program. To meet a cyber threat that will always evolve, we need to encourage a strong workforce to bring their talents to secure our online world.

- **Passing legislation improving the government's ability to deter, investigate, and prosecute cybercrime.** While many private-sector entities are making substantive efforts to manage their risks and protect their networks, intellectual property, and businesses, criminals continually evolve their tactics and are becoming much more sophisticated. The breadth of criminal activity and number of bad actors make getting ahead of them and crafting responses to incidents difficult. Cyberspace, with its global connectivity, poses considerable challenges to those tasked with protecting it. While the tools might be different from those used by criminals offline, those who wield them are criminals nonetheless. Leveraging and strengthening these laws and enforcement capabilities of law enforcement agencies to combat cyber crime will help to increase cybersecurity.

- **Passing effective cyber threat information-sharing legislation.** Lawmakers should focus on legislation improving cybersecurity threat information sharing in a way that protects privacy and offers adequate legal liability protection for businesses.

As I noted earlier in my testimony, threats will continue to evolve, and so must our responses. Thus, there will be changing needs for education, awareness, R&D, and legislation. In order to effectively and nimbly stay ahead of the threats, Congress must approach these challenges by employing flexible, risk-based approaches that are technology-neutral and foster robust public-private collaboration.

Conclusion

Members of the subcommittee, ITI and our member companies are pleased you are examining the important issue of cybersecurity in the 21st Century. As I said at the opening of my testimony, while the challenges are many, we also have an opportunity to get it right. The ICT industry is constantly innovating and is committed to addressing those threats. We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to collectively improve cybersecurity risk management and resilience.

Thank you.